IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

AMEDISYS HOLDING, LLC	)	
	)	
Plaintiff,	)	
	)	**Civil Action No. _____**
v.	)	
	)	
INTERIM HEALTHCARE OF ATLANTA, INC., DENISE CATHEY, BRENDA HOGAN, and JENNIFER MACK	)	**JURY TRIAL DEMANDED**
	)	
Defendants.	)	
_____	)	

MEMORANDUM OF LAW IN SUPPORT OF AMEDISYS HOLDING, LLC'S MOTION FOR A TEMPORARY RESTRAINING ORDER

INTRODUCTION

On April 18, 2011 three Amedisys Holding, LLC ("Amedisys" or "Plaintiff") employees—Jennifer Mack, Brenda Hogan, and Denise Cathey (the "Individual Defendants")—abruptly and without notice resigned and shortly thereafter began working for Interim Healthcare of Atlanta, Inc. ("Interim"). Less than a week before her resignation Mack, an Amedisys Care Transition Coordinator ("CTC") who had access to extensive confidential patient information, emailed from her Amedisys email account to her personal Yahoo account information regarding over 1,260 Amedisys patients or

prospective patients in direct violation of Amedisys policies and procedures and Health Insurance Portability and Accountability Act ("HIPAA") requirements. There was no legitimate business reason for Mack to email this highly sensitive patient information to herself other than to use it for the commercial benefit of herself and her new employer.

At the same time, Hogan, who was an Account Executive responsible for generating patient referrals by developing contacts and relationships with healthcare providers, failed to return to Amedisys upon her resignation an Account Executive's Territory Workbook (the "Workbook"). The Workbook contained trade secrets developed by a third party for, and at great expense to, Amedisys regarding the referral history and patterns of healthcare providers in the areas served by Hogan for Amedisys. There was no legitimate business reason for Hogan to retain this information other than to use it to benefit herself and her new employer.

During the weeks following their abrupt resignation, Mack, Hogan and, upon information and belief, Cathey have used the trade secrets and patient information they obtained while employed by Amedisys to compete with Amedisys for patient referrals from healthcare providers and healthcare facilities that they served while employed by Amedisys. Such use of Amedisys trade secrets is a misappropriation of trade secrets in violation of the Georgia Trade Secrets Act and should be prohibited. Specifically, because the functions performed by Mack and Hogan are substantially similar to those they were providing for Amedisys, it is inevitable that they must use the Amedisys trade

secrets to perform their jobs for Interim. Accordingly, they should be prohibited from soliciting patient referrals from any healthcare facility or provider or Amedisys patient or prospective patient with whom they had contact on behalf of Amedisys or about whom they obtained information while employed by Amedisys. In addition, defendants should be required to return all trade secrets and other property, including electronic copies of documents and patient information belonging to Amedisys as required by their Non-Solicitation Agreements.

FACTS

A. Amedisys's Business

Amedisys delivers home health care and hospice services to more than 35,000 patients and their families throughout the country. Because hospital and doctor referrals to their patients account for much of Amedisys's business, the company's success depends in large part on relationships with healthcare providers developed over time and at great expense to Amedisys by employees like the Individual Defendants. (Benton Decl. ¶ 13.) Account Executives (such as Hogan) at Amedisys focus their business development efforts on physician referrals. (McDonald Decl. ¶ 12.) Care Transition Coordinators ("CTCs") (such as Mack and Cathey) focus on referrals from hospital administrators readying patients for discharge. (*Id.*) In each case, the Amedisys employee devotes extensive time and effort, all at the expense of Amedisys, developing relationships with the representative healthcare providers and promoting the nature and

quality of Amedisys's services. (*Id.* ¶ 13.)

B. The Protected Information

Amedisys Account Executives and CTCs cultivate these crucial relationships by using, among other things, highly specific and confidential analyses of each geographic market, including Georgia, in which the company operates. These analyses include: (a) the Workbook, a statistical compilation provided by a third party for which Plaintiff pays a substantial fee; and (b) patient information created or received by Amedisys and maintained in Amedisys's proprietary computer databases (the "Referral Logs") (collectively, the Workbook and Referral Logs constitute the "Protected Information").

The Workbook compiles detailed home health care referral statistics for specific doctors in the territories where Amedisys operates. (Goldsmith Decl. ¶ 5.) The Workbook lists for example, the physician's name, practice, specialty, how often she refers patients for home healthcare services for various ailments (e.g., cardiac care, diabetic care, orthopedic care), to which home healthcare providers she refers her patients, and what proportion of that physician's total referrals each home healthcare provider captured over the last quarter. (Benton Decl. ¶¶ 3–5.) This information allows Amedisys Account Executives to effectively identify and prioritize the physicians on whom they should focus their efforts.

Amedisys spent over $900,000 to develop and purchase the Workbook and pays $50,000 per year for updated data. (Goldsmith Decl. ¶ 6; Benton Decl. ¶ 6.) It provides a

geographically specific Workbook to each Account Executive who works within each territory. (Benton Decl. ¶ 4.) Because the information contained in each Workbook is proprietary and would substantially benefit any competitor, Amedisys limits the Workbook's distribution to Account Executives assigned to each territory covered by that Workbook. (*Id.*) Each page of each Workbook carries as well the following designation: "All information contained herein is the confidential property of Amedisys. Recipients of this binder shall not disclose any of the information contained herein to any third party." (*Id.* ¶ 11.) The Workbook is distributed to each Account Executive through Amedisys's secure computer network. (*Id.* ¶ 10.)

Amedisys also creates and maintains Referral Logs that contain detailed information regarding current and prospective patients' referral dates, referral sources, physicians' names, contact information, patient numbers, assigned home health care agents, admittance and referral codes, and other protected health information. (McDonald Decl. ¶¶ 5–6.) Because the Referral Logs contain information concerning prospective patients, i.e., patients that are about to be discharged from inpatient care and have been determined eligible for home care, the Referral Logs represent Amedisys's "pipeline" for future business. (*Id.* ¶¶ 9, 11.) All Amedisys employees with access to the Referral Logs, or any other patient information, are required to sign a Health Insurance Portability and Accountability Act Confidentiality Covenant ("HIPAA Covenant"). Each of the Individual Defendants signed such an agreement. (Ex. A.)

C. Amedisys's Security and Confidentiality Measures for the Protected Information

Amedisys has imposed a variety of security measures to protect its trade secret and patient information such as the Workbooks and Referral Logs. The network on which the Protected Information was stored is protected from outside interference or access by two firewalls that are co-managed by Amedisys and an independent company. (Glover Decl. ¶ 4.) Employees who are authorized users of the Amedisys network must log in using a company-provided login ID and password. (*Id.* ¶ 5.) Once logged into the network, each employee only has access to pre-approved data that is determined by that employee's job title and responsibilities. (*Id.* ¶ 6.) Accordingly, when Amedisys pushes information onto network databases, permissions are set to prevent unauthorized employees from gaining access to sensitive data that are not required for their job responsibilities. (*Id.* ¶ 7.)

AMS, Amedisys's proprietary management system, further has its own security modules to prevent unauthorized use. With respect to Amedisys's email system, in addition to typical login credentialing, the Company runs two additional security components. An application called Trend IMSS monitors all outbound email from Amedisys's email system and flags messages with certain keywords and phrases. (*Id.* ¶ 9.) When such messages are identified, the message is not delivered to the addressee; instead, the addressee receives a hypertext link to a secure website called Authentica.

(*Id.* ¶ 10.) In Authentica, the addressee must register with the site with his or her email address and affiliation and only after doing so can the addressee view the message in a secure environment. (*Id.* ¶ 11.)

In addition to electronic security measures, Amedisys requires its employees to commit to keeping trade secrets and patient information such as the Workbook and Referral Logs confidential. Its employee handbook includes confidentiality, disciplinary, and duty of loyalty provisions, and non-disclosure covenants, to which the Individual Defendants were required to agree. (Ex. B.) These policies require employees to take affirmative steps to protect confidential information, including without limitation restricting employees' access to proprietary information based on that employee's position, limiting access to information to a need-to-know basis, and other steps. (Exs. B, C.) Each of the Individual Defendants also signed a confidentiality agreement prohibiting employees' disclosure of Amedisys patients' protected health information. (Ex. A.)

D. The Individual Defendants' Unauthorized Acquisition of the Protected Information

On or about April 12, 2011, and while employed by Amedisys, Mack used the secured email system to send Referral Logs containing information for over 1,200 Amedisys patients to her personal Yahoo email account. (Ex. D.) By doing so, Mack not only violated Amedisys's policies on confidentiality of electronic information, she also

violated the HIPAA prohibition against "obtain[ing] individually identifiable health information relating to an individual." 42 U.S.C. § 1320d-6(a)(2). Upon information and belief, Cathey, who works closely with Mack, also has access to the Referral Logs that Mack emailed to herself on April 12, 2011.

On or about April 1, 2011, and while still employed by Amedisys, an Amedisys employee sent Hogan an electronic copy of the Workbook for her territory through the Company's secured email system. (Benton Decl. ¶ 15.) Hogan printed and retained in hard copy this document and at least one earlier version of the Workbook.

Interim now employs the Individual Defendants in the same or substantially similar positions to those they held with Amedisys. Amedisys employees have seen each of the Individual Defendants soliciting in the same healthcare facilities as those they solicited on behalf of Amedisys since they began working for Interim. (Greenlow Decl. ¶¶ 4–6; Antonio Decl. ¶¶ 4–7.)

STANDARD OF DECISION

This Court may issue a temporary restraining order to preserve the status quo and prevent irreparable harm until a hearing can be held. Fed. R. Civ. P. 65; *SunTrust Bank v. Houghton Mifflin Co.*, 268 F.3d 1257, 1265 (11th Cir. 2001). The Court should issue the requested temporary restraining order if Amedisys can demonstrate: (1) a substantial likelihood of success on the merits; (2) irreparable harm in the absence of an injunction; (3) its harm absent an injunction will exceed Amedisys's harm from the injunction

requested; and (4) an injunction would serve the public interest. Fed. R. Civ. P. 65; *Davidoff & CIE, S.A. v. PLD Int'l Corp.*, 263 F.3d 1297, 1304 (11th Cir. 2001) (affirming grant of preliminary injunction); *see also Shiavo ex rel. Schindler v. Shiavo*, 403 F.3d 1223, 1225 (11th Cir. 2005); *Ingram v. Ault*, 50 F.3d 898, 900 (11th Cir. 1995) (TRO). Amedisys must make these showings by a preponderance of the evidence, and this Court will not be reversed absent clear error of law or abuse of its discretion. *Renteria-Marin v. Ag-Mart Produce, Inc.*, 537 F.3d 1321, 1324 (11th Cir. 2008) (affirming district court for absence of clear error, "which is a highly deferential standard").

ARGUMENT AND CITATIONS OF AUTHORITIES

I. AMEDISYS HAS A SUBSTANTIAL LIKELIHOOD OF SUCCESS ON THE MERITS

A. Defendants Mack and Hogan Violated the Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, provides a private cause of action against a person who, inter alia: "accesses a computer without authorization or exceeds authorized access," to obtain "information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). As described above, Amedisys has taken reasonable measures to maintain the Protected Information in a secure and confidential environment, and to ensure that its employees treat this information accordingly. (Benton Decl. ¶ 10; McDonald Decl. ¶ 8.)

Mack and Hogan thus obtained and retained the Referral Logs and Workbook after their resignations only by exceeding the authorization given them by Amedisys to use its protected computer network. While Mack may have been authorized to access the Referral Logs on April 12, she was not authorized to email them to herself or later use them to compete with Amedisys. Likewise, Hogan was not authorized to access the Workbook to print copies for her own personal use or use in competition with Amedisys. *See United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (affirming CFAA conviction for employee who accessed information for purposes not related to employer's business even though he was otherwise authorized to use such information within the scope of his employment); *United States v. Salum*, 257 F. App'x 225, 230 (11th Cir. 2007) (affirming CFAA conviction of employee who "exceeded his authority by accessing [employer's computer system] for an improper purpose").

Mack's and Hogan's actions have caused the Company losses well in excess of five thousand dollars. *See* 18 U.S.C. §§ 1030(a)(5)(B)(i); 1030(11) (defining "loss" as "any reasonable cost to the victim, including the cost of responding to an offense, conducting damage assessment, and restoring the data, program, system, or information to its condition prior to the offense . . ."). In addition to lost business from both misappropriations, Mack's Referral Log misappropriation violates HIPAA and requires that the Company mitigate the effects of the misappropriation. The cost of this effort will

far exceed $5,000 in addition to the attendant damage to Amedisys' business reputation. *See* 45 C.F.R. 164.530.

Courts routinely find that former employees who misappropriate employer data such as customer lists have violated CFAA. *E.g.*, *Keg Techs., Inc. v. Laimer*, 436 F. Supp. 2d 1364, 1380 (N.D. Ga. 2006) (issuing injunction under CFAA against former employee who misappropriated computer files containing employer's customer lists). Accordingly, the Company is substantially likely to succeed on the merits of its claim that the Individual Defendants violated CFAA. *See* 18 U.S.C. § 1030(g) (allowing injunctive relief for victims of CFAA violations); *see also Pac. Aero. & Elecs., Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1195 (E.D. Wash. 2003) (authorizing private cause of action by employer against former employees and their new companies who sought competitive edge through unauthorized removal of information or programs from employer's computer database).

B. Defendants Mack and Hogan Have Violated the Stored Communications Act

The Stored Communications Act imposes civil liability on anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains . . . a wire or electronic communication while it is in electronic storage." 18 U.S.C. §§ 2701(a), 2707. As set forth above, Mack and Hogan

exceeded their authorization to access and use Amedisys's computer information systems and used such access to obtain the Referral Logs and Workbook in electronic form. The Stored Communications Act prohibits this behavior. *See White v. Baker*, 696 F. Supp. 2d 1289, 1297 (N.D. Ga. 2010) (Stored Communications Act prohibits unauthorized access of electronic information). Accordingly, Amedisys has a substantial likelihood of success on this claim as well.

C. The Individual Defendants and Interim Have Misappropriated Amedisys's Trade Secrets

This Court may enjoin the actual or threatened misappropriation of trade secrets. O.C.G.A. §§ 10-1-760, 10-1-762(a). Amedisys therefore is entitled to an injunction to protect it from continued irreparable harm due to this misconduct by the Defendants.

1. The Protected Information Constitutes Trade Secrets

The Georgia Trade Secrets Act ("GTSA") defines a trade secret as confidential, proprietary information not commonly known by the public that "(A) [d]erives economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (B) [i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy." O.C.G.A. § 10-1-761(4)(A)-(B).

The Workbook and the Referral Logs derive economic value from not being generally known to or ascertainable by competitors. (McDonald Decl. ¶ 15; Benton Decl.

¶ 14.) Further, the GTSA explicitly makes such "method[s], . . . financial plans, and list[s] of existing or potential customers" protectable trade secrets. O.C.G.A. § 10-1-761(4).

Amedisys has undertaken reasonable efforts to maintain the secrecy of its trade secrets. As shown above, Amedisys allows the Workbook's and Referral Logs' transmission only via the Company's protected computer network and email system, to which access is limited and controlled. (McDonald Decl. ¶ 8; Benton Decl. ¶ 10.) Amedisys makes the Workbook available to only Account Executives who work with the specific geographic areas covered in the Workbook (Benton Decl. ¶ 4), and marks each page with the designation "All information contained herein is the ***confidential property of Amedisys***. Recipients of this binder shall not disclose any of the information contained herein to any third party." (*Id.* ¶ 11.) Thus, the Protected Information constitutes trade secrets. *See Elec. Data Sys. Corp. v. Heinemann*, 493 S.E.2d 132, 136 (Ga. 1997) (employer exercised reasonable care to protect its trade secrets through confidentiality agreements with employees and limiting access to the information).

2. The Individual Defendants and Interim Misappropriated Amedisys's Trade Secrets

Under the GTSA, a trade secret is misappropriated when it is "[a]cqui[red] . . . by a person who knows or has reason to know that the trade secret was acquired by improper means," or is "[d]isclos[ed] without express or implied consent by a person who . . .

[u]sed improper means to acquire knowledge of a trade secret . . . [or] [a]cquired under circumstances giving rise to a duty to maintain its secrecy or limit its use." O.C.G.A. § 10-1-761(2); *see also id.* § 10-1-761(1) (defining "improper means" as including "theft, bribery, misrepresentation, breach or inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use, or espionage through electronic or other means").

The Individual Defendants misappropriated Amedisys's trade secrets by each of the following actions, each of which constitutes a separate and distinct violation of the GTSA:

(1) Mack emailed the Referral Logs to her own personal email account;

(2) Cathey, upon information and belief, has access to and has used the Referral Logs Mack misappropriated;

(2) Hogan exceeded her authorization to use the Workbook by printing, keeping, and continuing to use it after resigning her position with Amedisys; and

(3) Interim hired Defendants Mack, Cathey and Hogan and permitted them to continue to use the Protected Information to benefit Interim.

The Individual Defendants obtained this confidential information in breach of their contractual and common law duties of confidentiality to Amedisys. (Ex. A; *DeKalb Collision Ctr., Inc. v. Foster*, 562 S.E.2d 740, 745 (Ga. Ct. App. 2002). All knew that

this information was maintained on secured computer systems. (Ex. C.) All knew that the Referral Logs contained Protected Health Information under HIPAA, and that each had a duty to keep such information confidential. (Ex. A.) Moreover, given that the "Protected Health Information" falls squarely into the statutory definition of trade secrets, *see* O.C.G.A. § 10-1-761(4) (protecting "list[s] of actual or potential customers"), Interim "kn[ew] or has reason to know that the trade secret was acquired by improper means," *id.* § 10-1-761(2). Additionally, the Individual Defendants are now employed by Interim in substantially similar positions to those they held with Amedisys, which means that their "new employment will inevitably lead [them] to rely on [Amedisys's] trade secrets," thereby further misappropriating such trade secrets. *PepsiCo v. Redmond*, 54 F.3d 1262, 1269 (7th Cir. 1995). Amedisys is thus substantially likely to succeed on its misappropriation of trade secrets claim against the Individual Defendants.

D. The Individual Defendants Have Breached Their Fiduciary Duties to Amedisys

The Individual Defendants owed Amedisys a fiduciary duty "of loyalty, faithful service and regard for an employer's interest" while they worked there. *DeKalb Collision Ctr.*, 562 S.E.2d at 745. Accordingly, they "may not make a profit for [themselves] out of the [agency] relationship, or out of the knowledge obtained from the relationship, to the injury of the principal." *Koch v. Cochran*, 307 S.E.2d 918, 919 (Ga. 1983) (internal quotation marks omitted). Nevertheless, the Individual Defendants copied and/or

downloaded Amedisys's trade secrets and patient information without authorization, and, upon information and belief, disseminated this information to Cathey and Interim, and are continuing to use the trade secrets and other confidential information to benefit themselves and harm Amedisys. Based on this wrongdoing alone, the Company is substantially likely to succeed on the merits of its claim that the Individual Defendants have breached fiduciary duties and duties of loyalty to Amedisys.

E. Defendants Mack and Hogan Have Breached Their Contracts

Defendants Mack and Hogan signed binding agreements with Amedisys in which they promised, in part, to return to Amedisys all confidential information owned by Amedisys at the termination of their employment. (Ex. E.) Because they did not do so, they are in breach of that contract, and Amedisys is substantially likely to succeed on its breach of contract claim.

II. AMEDISYS IS SUFFERING IRREPARABLE HARM, AND WILL CONTINUE TO SUFFER IRREPARABLE HARM WITHOUT AN INJUNCTION

The Individual Defendants have directly caused and, unless immediately enjoined by the Court, will continue to cause irreparable injury to Amedisys through misappropriation of its trade secrets, interference with its business operations, and loss of its competitive advantage. As the GTSA recognizes, such misappropriation is a *per se* irreparable harm. *See* O.C.G.A. § 10-1-762(a) (authorizing injunction because of its recognition that irreparable harm is inevitably caused by the disclosure or use of trade

secrets). In addition to the statutory scheme, courts routinely have held that the mere "[t]hreat of disclosure, destruction or dilution of [a] plaintiff's trade secrets constitutes irreparable injury justifying injunctive relief." *Specialty Chems. & Servs., Inc. v. Chandler*, 1988 WL 618583, at *5 (N.D. Ga. Sept. 29, 1988 (internal quotation marks omitted); *see also Mouldings, Inc. v. Potter*, 315 F. Supp. 704, 712 (M.D. Ga. 1970) (granting interlocutory injunctive relief after noting that the plaintiff had "developed processes, techniques, machinery, and customer and supplier relationships of a confidential nature, some of which are trade secrets, at great expense and effort, [thus permitting] plaintiff to acquire a limited competitive advantage over other companies engaged in the same business").

Moreover, Amedisys has invested substantial time and expense in creating, developing, and maintaining its trade secrets and patient information at issue in this case that was misappropriated through violations of CFAA, the Stored Communications Act, and breach of the Individual Defendants' fiduciary duties. The Protected Information is highly sensitive and would be of enormous economic value to the Company's competitors. (McDonald Decl. ¶ 14; Benton Decl. ¶¶ 14–15.) The Protected Information provides detailed information as to hundreds of customers to whom Amedisys has offered services and the sources of the referrals for those customers. (McDonald Decl. ¶ 5; Benton Decl. ¶ 3.) This information was compiled or purchased at great cost to Amedisys. (Benton Decl. ¶ 6; *see* McDonald Decl. ¶¶ 6–7.) The Workbook and Referral

Logs constitute Amedisys's "game plan," and Interim's unauthorized acquisition of this confidential material will give it an unearned advantage in the marketplace. Additionally, the Referral Logs that Mack copied without authorization contain HIPAA Protected Health Information for more than 1,200 Amedisys clients. (McDonald Decl. ¶ 15.)

III. THE BALANCE OF HARMS GREATLY FAVORS AMEDISYS

Amedisys seeks an order preventing the Individual Defendants from continuing to engage in illegal behavior, which, if it continues, will result in the disclosure of enormously valuable trade secrets belonging to the Company. The harm to Amedisys if the Court does not grant an injunction is extreme and irreparable. Indeed, given that wrongfully disclosed patient Protected Health Information under HIPAA is at issue, Amedisys clearly stands to suffer great harm in terms of negative publicity and injury to its business reputation if the Individual Defendants' are not enjoined.

Conversely, as this Court has recognized, a party "cannot suffer compensable harm when enjoined from unlawful activity." *Specialty Chem. & Servs., Inc.*, 1988 WL 618583, at *4 (granting motion for preliminary injunction). Thus, requiring the Individual Defendants to refrain from engaging in unlawful activity would not result in any undue or unfair harm to them. *See* 42 U.S.C. § 1320d-6(a) (creating criminal liability for anyone who "obtains individually identifiable health information relating to an individual"); *Lowe v. Vadlamudi,* 2010 WL 2474806, at *2 (E.D. Mich. June 14, 2010)

("HIPAA prohibits the wrongful disclosure of individually identifiable health information . . . .").

IV. THE PUBLIC INTEREST FAVORS AN INJUNCTION

Granting Amedisys's motion will advance the public interest. Indeed, the GTSA recognizes the public interest in protecting trade secrets by specifically providing for injunctive relief even for merely "threatened" disclosure of trade secrets. O.C.G.A. § 10-1-762(a); *see, e.g., DeGiorgio v. Megabyte Int'l, Inc.*, 468 S.E.2d 367, 369 (Ga. 1996); *Avnet, Inc. v. Wyle Labs., Inc.*, 437 S.E.2d 302, 304 (Ga. 1993). Enjoining the Individual Defendants from further misappropriation of Amedisys's trade secrets and highly confidential information and requiring the return of such information to Amedisys promotes this important public interest. Indeed, because HIPAA Protected Health Information has been compromised, Amedisys has an obligation to mitigate such disclosure, *see* 45 C.F.R. 164.530, putting the public interest squarely in favor of an injunction that prohibits further use. By contrast, there is no public interest in permitting the Individual Defendants to continue to unfairly profit at Amedisys's expense.

CONCLUSION

For the foregoing reasons, Amedisys respectfully requests that its motion be granted and that the Court issue a temporary restraining order against Defendants that (1) requires the Individual Defendants and Interim to return any and all trade secrets and other property, including documents and electronic copies of documents and patient

health information, belonging to Amedisys; (2) requires the Individual Defendants and Interim to submit to a forensic audit of their computer systems to be performed by a neutral third party to ensure that no trade secrets or electronic copies of documents belonging to Amedisys remain on any such computer systems; and (3) prohibits the Individual Defendants from soliciting business on behalf of Interim from patients, prospective patients, healthcare providers, or healthcare facilities of any nature with which they had contact or about which they obtained information while employed by Amedisys for a period of fourteen (14) days after the Court's order. A proposed order is attached.

Respectfully submitted this 4th day of May, 2011.

/s/ Michael W. Johnston
Michael W. Johnston
Ga. Bar No. 396720
mjohnston@kslaw.com
M. Russell Wofford
Ga. Bar No. 773002
rwofford@kslaw.com

KING & SPALDING LLP
1180 Peachtree Street
Atlanta, Georgia 30309
(404) 572-4600 (telephone)
(404) 572-5100 (facsimile)

COUNSEL FOR PLAINTIFF AMEDISYS HOLDING, LLC

LR 7.1 D CERTIFICATION

Counsel hereby certifies that the foregoing was prepared in Times New Roman, 14-point font, in accordance with LR 5.1 B.

/s/ Jason R. Edgecombe
Jason R. Edgecombe